ABSTRACT

ROUND KEY GENERATION FOR AES RIJNDAEL BLOCK CIPHER

Successive round keys of an expanded key according to the AES block cipher algorithm are generated from an initial cryptographic key, for use in a cryptographic (encryption and/or decryption) engine, in real time as the cryptographic process is executing. A limited key memory is used by overwriting previously generated words of the expanded key, leaving only the words of the initial key and the final key in the memory. Thus, a subsequent cryptographic operation can recommence either in the encryption or decryption direction, without delay to the cryptographic engine.

[Fig 3.]